DARPA-BAA-15-29
Brandeis
Frequently Asked Questions

As of April 15, 2015

Q32: Will TA4 performers be expected to interact with and assess all TA3 performers/systems, or just selected subsets?

A32: TA4 performers would interact with TA3 subsets.

Q31: Is it the responsibility of TA4 or TA3 performers to generate data or orchestrate experiments needed to properly support privacy measurement and assessment?

A31: It is the responsibility of TA3 performers to generate data sufficient for TA1 and TA2 performers to work effectively. Depending on the TA4 techniques proposed it may be the responsibly of the TA4 performer to orchestrate experiments needed to properly support privacy measurement and assessment.

Q30: Do we need to specify individual versus enterprise-focused concepts?

A30: No, you don't need to specify it. It would be fine either to have something which really focuses on personal privacy, or on collective privacy, or has elements of both.

Q29: Will you entertain hardware solutions or hardware-software solutions?

A29: Absolutely. Hardware solutions are not ruled out. If that's the way to make the thing work and you can make a compelling case for it, and then make that case.

Q28: Can FFRDCs participate as subs?

A28: FFRDCs and Government entities (e.g., Government/National laboratories, military educational institutions, etc.) are subject to applicable direct competition limitations and cannot propose to this solicitation in any capacity unless the following conditions are met.

FFRDCs must clearly demonstrate that the proposed work is not otherwise available from the private sector and must provide a letter on official letterhead from their sponsoring organization citing the specific authority establishing the FFRDC's eligibility to propose to Government solicitations and compete with industry, and compliance with the terms and conditions in the associated FFRDC sponsor agreement. This information is required for FFRDCs proposing as either prime contractors or subcontractors.

Government entities must clearly demonstrate that the proposed work is not otherwise available from the private sector and provide documentation citing the specific statutory authority (and contractual authority, if relevant) establishing their eligibility to propose to Government solicitations.

At the present time, DARPA does not consider 15 USC § 3710a to be sufficient legal authority to show eligibility. For some entities, 10 USC § 2539b may be the appropriate statutory starting point; however, specific supporting regulatory guidance, together with evidence of agency approval, will still be required to fully establish eligibility.

DARPA will consider eligibility submissions on a case-by-case basis; however, the burden to prove eligibility for all team members rests solely with the proposer.

Q27: Are there any restrictions regarding bidding or being selected for multiple technical areas?

A27: No. There are no restrictions.

Q26: To what extent is TA4 expected to be a privacy red team, i.e., a post development assessment of system privacy properties versus a more integral part of the system development.

A26: It would be interesting if TA4 had elements of both.

The primary issue is not just how systems are measured. Instead, how do we go in and solve the access problem to a system? What do we mean that a system is privacy-preserving? Could you even imagine a privacy crash rating on systems that gave you a sense of the capabilities of the system versus the privacy risks that was incurred?

Q25: What role can or should system building play in a TA1 proposal, or is TA1 focused just on developing technologies in the abstract, leaving implementation entirely to a TA3 performer?

A25:

What is envisioned is that we will have a collaborative team that is building the systems, and the TA3 performers have particular responsibilities as they're building the systems. TA1 will have other responsibilities as they're building the systems, TA2 will have other responsibilities as they're building systems, and the same with TA4.

So everybody's coming at it with responsibility for building the systems, but they just have different roles within that responsibility.

Q24: Can a proposal be across multiple TA's -- e.g., TA1 and TA3?

A24: No. The BAA goes into some detail on that.

Q23: For TA 1, the privacy-preserving computations, do you consider system-based, e.g., anti-tracking web browser, besides those traditional algorithm-based privacy-preserving techniques?

A23: The first order that we're trying to deal with is if a system where information needs to be shared with you to get the job done, how is this done without losing control of that information that is provided? That's the primary problem that the program is trying to address.

Q22: To what extent are you interested in tagging and provenance tracking?

A22: The goal is not to develop the techniques themselves, but to figure out how to build systems using an interesting variety of these techniques, and move our ability to build privacy-preserving systems forward.

Q21: Is there a concern with ID-bounded data or non-ID-bounded data or both? In other words, data that is bound to the identity of the person that it comes from.

A21: The answer to this is going to be entirely dependent on the needs as it fits within the systems that are being built.

Q20: Is it preferred to have an industry partner in the team?

A20: There is no preference one way or the other, as teaming compilation is completely up to the proposer. If it's a university team, do bear in mind that this is going to be a contract in all likelihood, so that means that it is anticipated that there will be required deliverables. So if that's impossible for you to do, but you've got some things that you could do if you worked with an industry team, then that would be your strategy to managing the contractual requirements.

Conversely, if you're an industry team, and you were just planning to crank the handle and you're not actually bringing any great ideas, then you may not be fulfilling the goals and objectives of the program. So if you find that you're not bringing any great ideas, you might want to think about partnering with somebody who might be able to bring great ideas.

Q19: How many awards are anticipated for each TA, and what's the expected size of award?

A19: The total amount of the budget is described in the BAA. It is anticipated that at least two, or maybe three, of these collaborative research teams will be formed. And each of them would have some TA1, TA2 and TA4 performance attached to them. Multiple awards are anticipated. The level of funding for individual awards made under this solicitation has not been predetermined and will depend on the quality of the proposals received and the availability of funds.

Q18: Some areas of relevant basic research were noted in passing during the BAA presentation, but it would be helpful to have some additional citations of basic research that would help guide what is in and out of scope for TA1 and TA2. Could some be provided with the understanding, of course, that they're non-exhaustive?

A18: It's very hard to give more guidance here. The reason is that TA1 and TA2 are not about the privacy-preserving computations or about human data interaction themselves, per se. It is about how we develop these techniques that we can use in systems. So it really has to be tied to application.

Q17: It was mentioned that the Brandeis program is not focused on cyber security. However, the sensitivity of user and network data is a significant obstacle to effective cooperation for cyber defense. Is the application of privacy-preserving computation techniques to cyber security of interest to Brandeis?

A17: There's the cyber security of the systems we build, and there's cyber security as an application domain that we may be building systems to inform the application domain.

The first of those is out of scope. The second of those is definitely in scope. And the application domains are not limited.

Q16: Since TA3 is an integration effort, can you say more about the boundary between TA3 and TA1, and TA2, given the requirement to only propose for one or the other? Here are two interpretations.

A TA 3 proposal could include a few TA1 and TA2 components, but would clearly describe how they would integrate with other components. Or a TA3 proposal would not include any TA1 or TA2 components, and only consist of a component-free integration framework?

Which of these (or something else) would you prefer??

A16: Regarding TA3, integration is part of it, but it would be a mistake just to think of TA3 as a system integrator, pulling stuff from other people.

There's going to definitely be some sort of co-engineering that goes on with TA1 and TA2 performers as the system is being built. TA3 work may even include helping to put in hooks for TA4. TA3 definitely are the integration points of all of that work, and so there is definitely an integration part of it. But the whole system conception is also involved in this.

Of these two in the sub-bullets, DARPA is much more inclined towards the second one. That is, if you have in mind a particular system and some TA1 or TA2 components, then you should be writing separate proposals. And in your team concept section, you can certainly describe how some of these things would fit together.

Q15: What sort of users are targeted by this development-- government, Department of Defense, or private-- and how might this work be transitioned to those users?

A15: There is no pre-conception on the sort of users that may be interested in what is produced by this program.

This is a program that is pushing forward the technology for different ways of thinking about data privacy and managing it in practice. It's not about building a system that somebody is going to use. So it may be that the things that we build, somebody says, that's relevant, and I could use that directly. In which case, obviously, DARPA would then work to transition it.

Q14: Where and how does the efficiency of the techniques presented in TA1 get evaluated?

A14: Given that DARPA is aiming ultimately to bring some of these techniques to bear on existing systems, we don't want to end up with a system that we've applied these privacy technologies to that somebody says, well, it's interesting in principle, but it it's disappointing because it runs so poorly.

There is no *a priori,* particular performance things for you to jump over, but they need to be that when these technologies are going into systems, that they work well enough for the systems themselves to still be credible and to still be a compelling case that somebody else might look at it and understand how to take these ideas and apply them to any system.

Secondly, TA4, when they're doing their measurements, it can be envisioned that part of a TA4 proposal is to assess how well some of these things are performing in terms of the cost, as well as their loss of information. When you're doing privacy-preserving things, the quality of the information sometimes gets degraded.

So there is an interest in having those kinds of measurements coming from TA4. This is not an evaluation in a formal sense. There is not a government evaluation team ; but we definitely will be getting feedback within the team all the time on things like performance.

At this time, there is not a plan to have any kind of down-select. The plan is to construct the team of all the sets of performance, and then have all performers move forward as collaborative research teams for the life of the program.

The BAA makes this clear, and if it is concluded that somebody simply is not making any worthwhile progress or they're not collaborating effectively, DARPA still has complete reedom on a case-by-case basis to change funding decisions.

Q13: Can you confirm that TA2 applies to both the individual and the enterprise scenario?

A13: Yes. There is interest in TA2 being applicable in both of those settings.

Q12: Can you please clarify proposers in TA2 should propose specific approaches for addressing HDI-- that's human data interaction-- in practice, including describing how their research will be tuned to the needs of a larger collaborative research team?

A12: So as with all of the technical areas, ultimately when we start working on the program, even though each of the technical areas and each of the proposal groups will be doing work on their own; it will be very much in the context of this collaborative research team that's put together. And cross-team collaboration will be a significant part of how we actually collectively do something which is more than just what one team or another team can do by themselves.

Q11: Are approaches of natural language input appropriate for TA2, either for passing existing policies or to clarify in a dialogue with the user?

A11: Without specific context, it is difficult for DARPA to assess appropriateness. It's certainly allowable. If you're talking about a setting where some level of natural language communication with the user is the way that you want to do that communication, then DARPA is fully open to that.

Q10: In TA2 research challenges, in the second bullet it mentions including embedded devices having no interfaces in the traditional sense. Is the idea for such embedded devices to only be data consumer or also data producer and this potentially owner of private data?

A10: DARPA recognizes some devices might be a data producers. So it might be part of your internet of things at home, for example, that are producing data all the time, but they don't have a traditional keyboard and screen kind of interface or mouse or anything like that.

So if you propose research into embedded devices, you may need to think about how do I communicate to an embedded device, the privacy choices.

Q9: In TA2 research challenges, the second bullet says interfaces for capturing privacy intentions that convey privacy implications in the data space. I'm sure the bullet didn't say quite that. Is it correct that this refers to capturing the privacy intentions of the user?

A9: Yes. It refers to capturing the privacy intentions of the user.

Does it also refer to privacy intentions of services or devices that consume and process data, possibly store data, and produce computational results about that data?

Absolutely. The BAA makes no distinction between whether the machine is holding some of your data and submitting it for you versus you providing that data directly. It's your data from your machine. You may need to be able to cover both kinds of it.

It's important for proposers, when you're thinking about TA2 and similarly TA1, not to just have your mind narrowly on that technical area. But you need to be thinking about what kind of system would this be used in and how would it be used. DARPA’s interest in TA1 and TA2 is not on pushing the science and the techniques themselves, but how we build systems bringing these perspectives to bear on the systems.

Q8: Is the scope of TA2 limited to privacy that is enforced through privacy-preserving computation, or should TA2 also be concerned with exchanging information in the clear?

A8: Consider information exchange as a spectrum. There exists a number of different kinds of technologies for doing privacy-preserving computation, and one of them is sharing things in the clear. It doesn't preserve a lot of privacy. But if you think of there being a scale, that's just one end of the scale.

So when somebody is saying how they want their data to be conveyed, one of the things might be, sure, I don't mind them knowing in what year I was born . And then that piece will be communicated in the clear.

It needs to talk about that right through to the other end of this piece of date -- my social security number, I don't want them to even know a single digit of it, but I do want the computation to proceed as if they have that data.

Q7: Does TA2 include cognitive behavioral modeling and analysis, or is the scope solely focused on secure computation techniques?

A7: At the highest level, TA2 is trying to do trying to span different abstraction levels. At the highest level you probably need to do something about understanding how the human being is thinking, so there may well be elements of this kind of thing there.

At the lowest level you need to be able to tell the TA3 and the TA1 people what they should be doing with their data, so it needs to be able to hook down at that level. The challenge of TA 2 is that there is this vast gulf that you're trying to span between.

It really is a bridging technical area. It's not study one end or study the other.

Q6: Is it OK to produce human subject experiments for TA2? If yes, in any phase, or only starting in phase two or three? If yes, is there an expectation to limit the budget of human subject experiments, e.g., and percentage of proposal value?

A6: Yes, it is OK to propose human subject experiments. That will not have your proposal determined non responsive. However, you should take into account that TA2 is not envisioned as being primarily about human subject experiments.

DARPA does not envision the need for human subject experiments, but if you make a compelling case that some piece of what is happening in TA2 really needs it, then DARPA is open to consideration.

If you intend to propose human experimentation, then there are major processes to go through, including institutional review boards, and that process is lengthy. As stated in the BAA, DoD/DARPA funding cannot be used toward HSR until all approvals are granted, so you should take all of that into account when figuring out cost and time tables.

Q5: Does TA3 include also coming up with test scenarios and evaluate data -- and I think evaluation data sets? Can TA3 focus only on the individual or only on the enterprise scenario?

A5: What about test scenarios and evaluation data sets?

So it's not TA3's job to measure the privacy of a system. That's TA4's job. But it is TA3's job to make sure that the system that we build is working appropriately. And so to the extent that that requires test scenarios and things like that, then absolutely.

A TA3 proposal may address either the individual or the enterprise scenario or have some sort of blend of both.

DARPA’s expectation is that that may be done through a number of the different collaborative research teams. But if you have an idea that very naturally gives elements of both, that does not prohibit it at all.

Q4: What set of services should the framework in TA 3 handle? Should it assume already a certain set of approaches for TA 1 such as secure computation and facilitate for those, or should it just demonstrate general capabilities for the framework?

A4: All of the technical areas have something of a challenge in that the BAA calls for you to envision how to work together with a team that's not yet been created. And so that's true for TA3, as much as it's true for any of the other teams.

Proposers need to show that they've got some great ideas that are of interest to DARPA, but that they’ve also got flexibility to tune to whatever the particular end proposals and collaborative teams that are put together.

Q3: Can one institution be part of multiple proposals in the same TA, in the same technical area?

A3: Yes.

Q2: Can a non-US institution be a prime?

A2: Yes. Non-U.S. organizations and/or individuals may participate to the extent that such participants comply with any necessary nondisclosure agreements, security regulations, export control laws, and other governing statutes applicable under the circumstances.

Q1: What's the expected size for teams in terms of organization or budget for the different TAs?

A1: There is no expected size, as it is unknown what may be proposed.